Algebraische Strukturen Teil 2

Algebraische Strukturen

Algebraische Strukturen:

- Gruppen
- Ringe
- Körper
- heute: *Vektorräume*

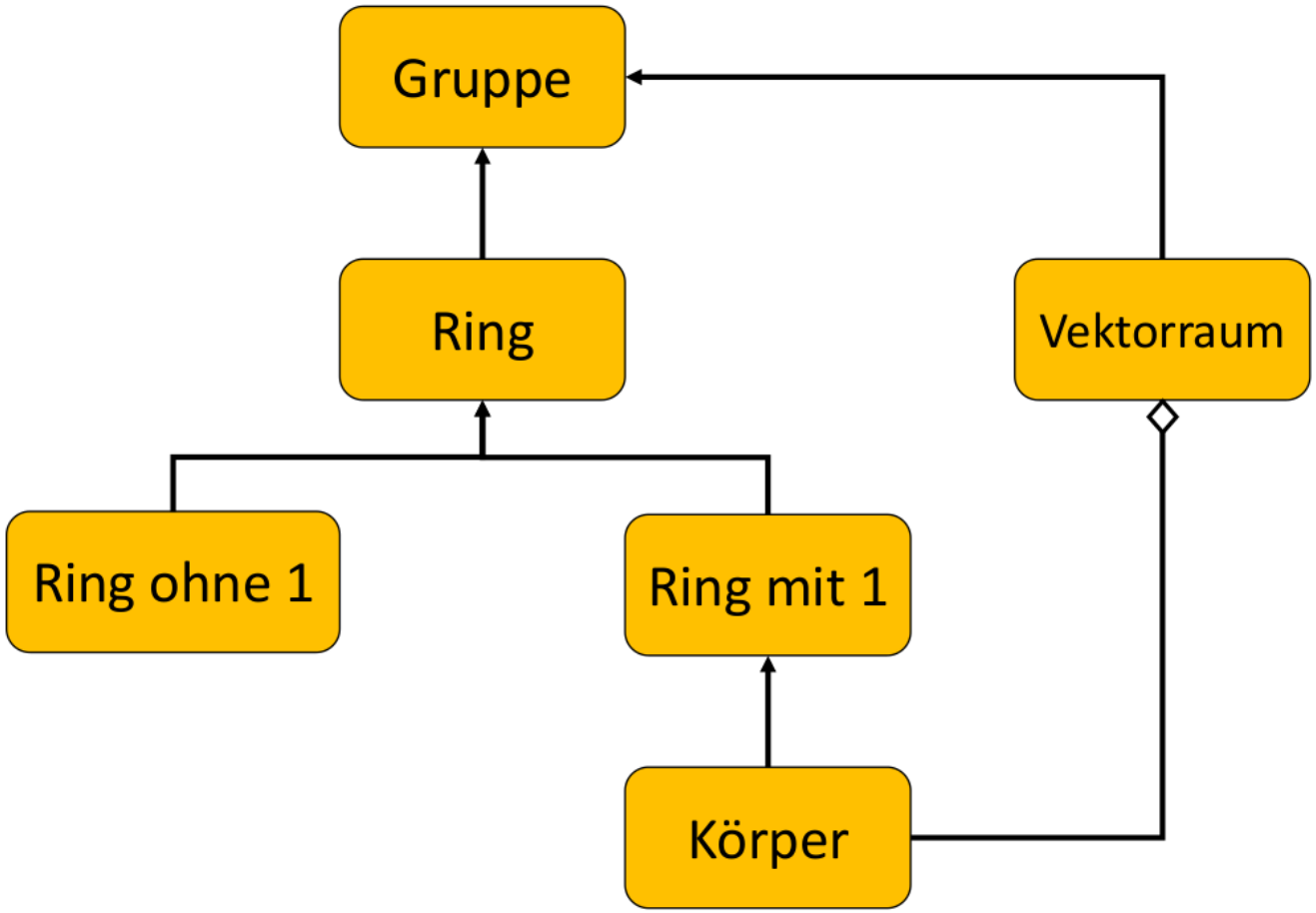
Außerdem:

- *Polynomdivision: Division mit Rest in Polynomringen über einem Körper K*
- *Homomorphismen: Abbildungen zwischen algebraischen Strukturen*

Anwendungen:

- *Reed Solomon: fehlerkorrigierende Codes*

Übersicht über algebraische Strukturen



Polynom-Ringe

Definition:
Sei R ein Ring mit $a_0, a_1, \ldots, a_n \in R$. Die Abbildung

$$f : R \to R, x \mapsto a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0$$

heißt **Polynom(funktion)** über R. Wenn $a_n \neq 0$ ist, ist n der **Grad** von f.

Ein Polynom ist eine altbekannte Sache, wenn man unter R $\mathbb{R}$ versteht, zB $f(x) = x + 1$ oder $f(x) = x^3 + 3 \cdot x^2 - 2$.

Polynom-Ringe

Ein Polynom macht aber (alleine) noch keinen Ring:

Definition:
Sei R ein Ring und wir bezeichnen die Menge aller Polynome über R mit $R[X]$. Wir haben die Verknüpfungen $+$ und $\cdot$ folgendermaßen definiert:

$$(1)\quad p + q = (p + q)(x) := p(x) + q(x)$$
$$(2)\quad p \cdot q = (p \cdot q)(x) := p(x) \cdot q(x)$$

$R[X]$ heißt dann **Polynomring** über R.

Polynomdivision

Polynomdivision

In den reellen Zahlen ist Division nicht besonders schwierig. Im Polynomring ist Division etwas schwieriger, aber auch hier funktioniert es. Zuerst: Über was reden wir genau?

Satz:
Sei K ein Körper, $K[X]$ der Polynomring über K. Dann gibt es für $f, g \in K[X]$ $(g \neq 0)$ $q, r \in K[X]$, sodass gilt $f = q \cdot g + r$ und $grad(r) < grad(g)$.

Polynomdivision

Erinnern wir uns zuerst nochmal wie Division funktioniert:

$$
\begin{array}{r}
285 : 9 = 31 \\
\underline{-27} \\
15 \\
\underline{-9} \\
6
\end{array}
$$

Die Aussage hier ist: $285 = 9 \cdot 31 + 6$.
Das ist dem vorherigen Satz nicht unähnlich. Wir haben etwas großes (285) in das Produkt zweier Zahlen plus einen kleineren Rest aufgespalten.
Polynomdivision funktioniert nun gar nicht so anders

Polynomdivision

Wir erinnern uns an die Schule:

$$
\begin{array}{l}
(x^3\text{-}5x^2\text{+}10x\text{-}8) : (x\text{-}1) = x^2\text{-}4x\text{+}6 \\
\underline{-(x^3\ \ -x^2)\qquad\qquad\qquad\quad} \\
\qquad -4x^2\text{+}10x\text{-}8 \\
\underline{\quad -(-4x^2\ \ +4x)\qquad\quad} \\
\qquad\qquad\qquad 6x\text{-}8 \\
\underline{\qquad\qquad\quad -(6x\text{-}6)} \\
\qquad\qquad\qquad\quad -2
\end{array}
$$

Wir sehen: Das Prinzip hier ist quasi dasselbe. Wir spalten ein großes Polynom in das Produkt zweier kleinerer und einen Rest auf:
$x^3 - 5x^2 + 10x - 8 = (x^2 - 4x + 6)(x - 1) - 2$
Insbesondere: Grad(-2)<Grad$(x - 1)$

Polynomdivision

Probiers mal selber:

$$(3x^3+2x-5) : (x^2+2x-1) = ?$$

Polynomdivision

Lösung:

$$
\begin{array}{l}
(3x^3 \quad +2x-5) : (x^2+2x-1) = 3x-6 \\
\underline{-(3x^3+6x^2-3x)} \\
\quad -6x^2+5x\ -5 \\
\underline{\quad -(-6x^2-12x+6)} \\
\quad 17x-11
\end{array}
$$

Polynomdivision

Sehr interessant sind diejenigen Divisionen bei denen der Rest gleich 0 ist:
Dh, wir haben ein Polynome f, sodass gilt $f = q \cdot g$ für zwei Polynome q, g mit kleinerem Grad als f
Z.B. wir können $(x^2 - 1)$ in $(x + 1)(x - 1)$ ohne Rest zerlegen, wie wir leicht nachrechnen können.

Satz
Wenn f eine Nullstelle x_0 hat, d.h. es gilt $f(x_0) = 0$, so ist f durch $(x - x_0)$ ohne Rest teilbar, d.h. $f(x) = (x - x_0) \cdot q(x)$.

Das bedeutet, wir haben die Nullstelle x_0 abgespalten!

Polynomdivision

Beweis:

Zu zeigen:
Wir haben f mit einer Nullstelle x_0. Die Behauptung ist nun, dass wir f aufspalten können in ein Polynom $(x - x_0)$ und einem unbekannten Polynom q mit Rest 0

Ausgeschrieben:
$f(x) = (x - x_0) \cdot q(x)$

Polynomdivision

Beweis:

Wir wissen $f(x) = (x - x_0)q(x) + r(x)$ und $\text{Grad}(r(x)) < \text{Grad}(x - x_0) = 1$.

Da $\text{Grad}(r(x)) = 0$ gilt, ist $r(x) = a_0 x^0 = a_0$ konstant.

Also: $f(x) = (x - x_0)q(x) + a_0$

Wir wissen $f(x_0) = 0 \Rightarrow 0 = f(x_0) = (x_0 - x_0)q(x_0) + a_0 = a_0$

$\Rightarrow f(x) = (x - x_0)q(x)$

Polynomdivision

Wir haben nun bei f eine **Nullstelle abgespalten**.
Wir wissen, dass das in $\mathbb{R}$ nicht immer geht, so können wir etwa bei $x^2 + 1$ keine Nullstelle abspalten.
Es wäre sonst nämlich $x^2 + 1 = 0 \Leftrightarrow x^2 = -1$ und das ist in $\mathbb{R}$ nicht definiert.

Aber: $x^2 = -1$ ist in $\mathbb{C}$ definiert! Und zwar mit $x = \pm i$. Wir können f über $\mathbb{C}$ betrachten ($\mathbb{C}$ ist ja nur die Erweiterung von $\mathbb{R}$ um i). In $\mathbb{C}$ zerfällt f also in $(x - i)(x + i)$. Da ein Polynom vom Grad 2 maximal 2 Nullstellen hat, können wir f nicht weiter aufspalten.

Merke: In $\mathbb{C}$ gilt: Wir können jedes Polynom in Polynome vom Grad 1 aufspalten. Das bedeutet es wenn wir sagen, dass $\mathbb{C}$ **algebraisch abgeschlossen** ist.
$\Rightarrow f = a_0(x - x_0)(x - x_1) \cdots (x - x_n)$

Homomorphismen

Homomorphismen

Definition:
Sind G und H Gruppen und $\varphi : G \to H$ eine Abbildung mit der Eigenschaft

1) $\varphi(a * b) = \varphi(a) * \varphi(b)$ für alle $a, b \in G$

dann heißt φ **(Gruppen-)Homomorphismus**.

Homomorphismen

Definition:
Sind R und S Ringe und $\varphi : R \to S$ eine Abbildung mit den Eigenschaften

1) $\varphi(a \oplus b) = \varphi(a) \oplus \varphi(b)$ für alle $a, b \in R$
2) $\varphi(a \odot b) = \varphi(a) \odot \varphi(b)$ für alle $a, b \in R$

dann heißt φ **(Ring-)Homomorphismus**.

Homomorphismen

Beispiele:
Betrachten wir die Abbildung $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, dh $z \mapsto z \bmod n$.
Wenn wir etwa $n = 5$ haben, dann: $\varphi(18) = 3$, $\varphi(35) = 0$

Satz:
φ ist ein Homomorphismus:

Beweis:
Sei $a = q_a n + r_a$ und $b = q_b n + r_b$:

$$\varphi(a)\varphi(b) = (a \bmod n)(b \bmod n) = r_a r_b$$
$$\varphi(ab) = \varphi((q_a n + r_a)(q_b n + r_b)) =$$
$$\varphi(q_a q_b n^2 + (r_a q_b + r_b q_a)n + r_a r_b) = r_a r_b \bmod n$$

Da wir uns in Restklassen bewegen, müssten wir noch zeigen
$[r_a r_b] = [r_a r_b \bmod n]$, aber das ist quasi die Definition.
Für Addition funktioniert der Beweis analog.

Homomorphismen

Beweise:
Für einen Homomorphismus $\varphi : G \to H$ gilt immer

a) $\varphi(e_G) = e_H$

Das neutrale Element wird immer auf das neutrale Element abgebildet.

b) $\varphi(a^{-1}) = \varphi(a)^{-1}$

Der Homomorphismus bewahrt die Inversen-Eigenschaft.

Homomorphismen

Beweis:

a) Zu zeigen: $e_H = \varphi(e_G)$

$e_H = \varphi(e_G) \odot \varphi(e_G)^{-1}$ // Def. neutrales Elt. e_H

$= (\varphi(e_G) \odot \varphi(e_G)) \odot \varphi(e_G)^{-1}$ // Def. neutrales Elt. e_G

$= \varphi(e_G) \odot \varphi(e_G) \odot \varphi(e_G)^{-1}$ //Def. Homomorphismus

$= \varphi(e_G) \odot e_H$ // Def. neutrales Elt. e_H

$= \varphi(e_G)$

Homomorphismen

Beweis:

b) Zu zeigen: $\varphi(a^{-1}) = \varphi(a)^{-1}$

Für $a \in G$ gilt:

$e_H = \varphi(e_G) = \varphi(a \odot a^{-1})$ //Def. inverses Elt.

$= \varphi(a) \odot \varphi(a)^{-1}$ //Def. Homomorphismus

$e_H \odot \varphi(a^{-1}) = \varphi(a)^{-1}$ //multipliziere mit $\varphi(a^{-1})$

$\varphi(a^{-1}) = \varphi(a)^{-1}$ //Def. neutrales Elt.

Homomorphismen

Definition:
Seien $(G, +)$ und $(H, +)$ Gruppen oder Ringe und $\varphi : G \to H$ ein Homomorphismus. Dann heißt

$$\text{Ker } \varphi := \{x \in G | \varphi(x) = 0\} \textbf{ Kern} \text{ von } \varphi,$$
$$\text{Im } \varphi := \{y \in H | \text{existiert } x \in G : \varphi(x) = y\} \textbf{ Bild} \text{ von } \varphi.$$

Anmerkung: Ker ist die Abkürzung von Kernel und Im von Image.

Ein bijektiver Homomorphismus heißt **Isomorphismus**.

Homomorphismen

Beispiel:
$5\mathbb{Z} := 0, 5, 10, 15, \ldots$.
Wir betrachten $\varphi : (\mathbb{Z}, +) \to (5\mathbb{Z}, +)$, $z \mapsto 5z$

Es gilt:
1) φ ist ein Homomorphismus:
$\varphi(a + b) = 5(a + b) = 5a + 5b = \varphi(a) + \varphi(b)$

2) injektiv: Für alle $c \in 5\mathbb{Z}$ gilt: Es gibt höchstens ein $a \in \mathbb{Z}$, sodass gilt $a \cdot 5 = c$.

3) surjektiv: Für alle $c \in 5\mathbb{Z}$ gilt: Es gibt ein $a \in \mathbb{Z}$, sodass gilt $a \cdot 5 = c$.

4) $\Rightarrow$ Im $\varphi = 5\mathbb{Z}$

5) Ker $\varphi = 0$

Anwendung: Reed Solomon

Allgemein

Reed Solomon Codes sind blockbasierte fehlerkorregierende Codes mit einem weiten Anwendungsfeld in digitaler Kommunikation, z.B. bei verschiedenen Speichermedien wie CD's, DVD's und QR Codes aber auch High-speed Modems wie ADSL und Satelliten Kommunikation.

- Reed-Solomon **Encoder** verwenden digitale Datenblöcke und fügen extra redundante Bits hinzu, da während der Übertragung Fehler entstehen können.
- Der Reed-Solomon **Decoder** verarbeitet jeden Block anschliessend und versucht die Fehler zu korregieren.

Galois Körper im Reed Solomon Code

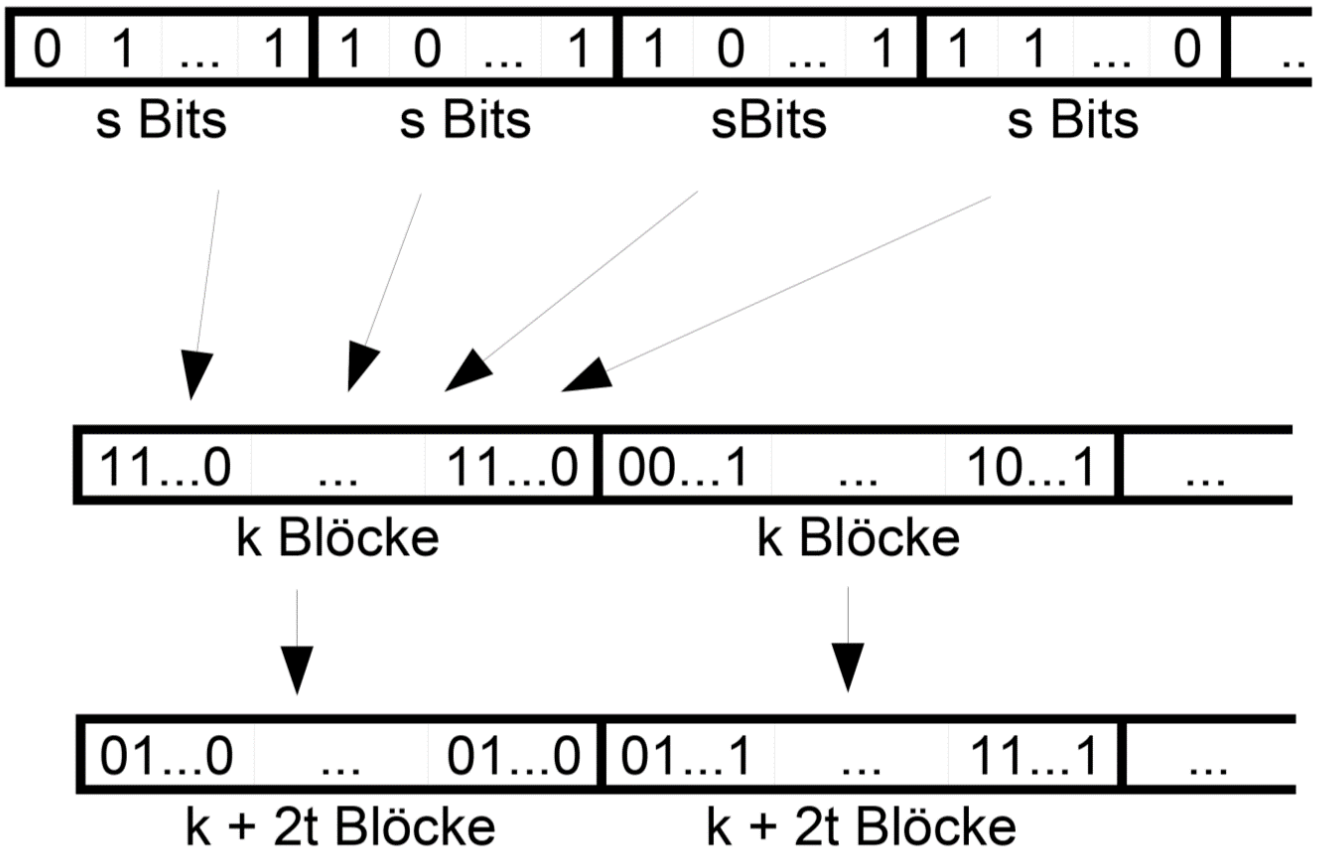
Wähle 3 Parameter:

- Alphabetgröße s,
- Blockgröße k,
- Fehlerrate t.

Relativ frei wählbar. Wichtig: $k + 2t \leq 2^s$

Alphabet für die Codierung sind die Elemente des Körpers $GF(2^s)$.

Übersicht Codierung



Algorithmus Codierung (Grundprinzip)

1. Einteilung der Quelldaten in k Zeichenketten der Länge von je s Bits
2. Bijektive Abbildung dieser Zeichenketten auf die Elemente von $GF(2^s)$
3. Erzeugung eines Polynoms des Grads $k-1$ aus der Folge von Elementen
$$p(x) = a_{k-1}x^{k-1} + ... + a_1x + a_0$$
4. Erzeugung eines Polynoms vom Grad $2t$, man nennt es auch das Generatorpolynom:
$$g(x) = (x-\alpha) \cdot (x-\alpha)^2 \cdot, ... \cdot (x-\alpha)^{2t}$$
5. Erzeugung des Polynoms $d := p(x) \cdot g(x)$
6. Abbildung der Koeffizienten von $d(x)$ auf die jeweiligen Bitfolgen

Bijektive Abbildung in $GF(2^s)$ mit $s = 4$

ord	Polynomdarstellung	Tupel (Bitsequenz)
0	0	0000
α^0	1	1000
α^1	x	0100
α^2	x^2	0010
α^3	x^3	0001
α^4	$1 + x^3$	1001
α^5	$1 + x + x^3$	1101
α^6	$1 + x + x^2 + x^3$	1111
α^7	$1 + x + x^2$	1110
α^8	$x + x^2 + x^3$	0111
α^9	$1 + x^2$	1010
α^{10}	$x + x^3$	0101
α^{11}	$1 + x^2 + x^3$	1011
α^{12}	$1 + x$	1100
α^{13}	$x + x^2$	0110
α^{14}	$x^2 + x^3$	0011

Algorithmus Decodierung (Grundprinzip)

1. Lese die Zeichenfolge ein und interpretiere sie als Polynom $f(x)$
2. Überprüfe auf Fehler: wenn keine Fehler, dann gilt $f(x) = d(x)$. Da $d(x)$ durch Multiplikation aus $p(x)$ und $g(x)$ entstanden ist gilt wenn kein Fehler vorliegt:

$$\forall i = 1, .., 2t : f(\alpha^i) = 0$$

3. Fehlerkorrektur ist möglich bei maximal t Fehlern:

$$f(x) = d(x) + e(x)$$

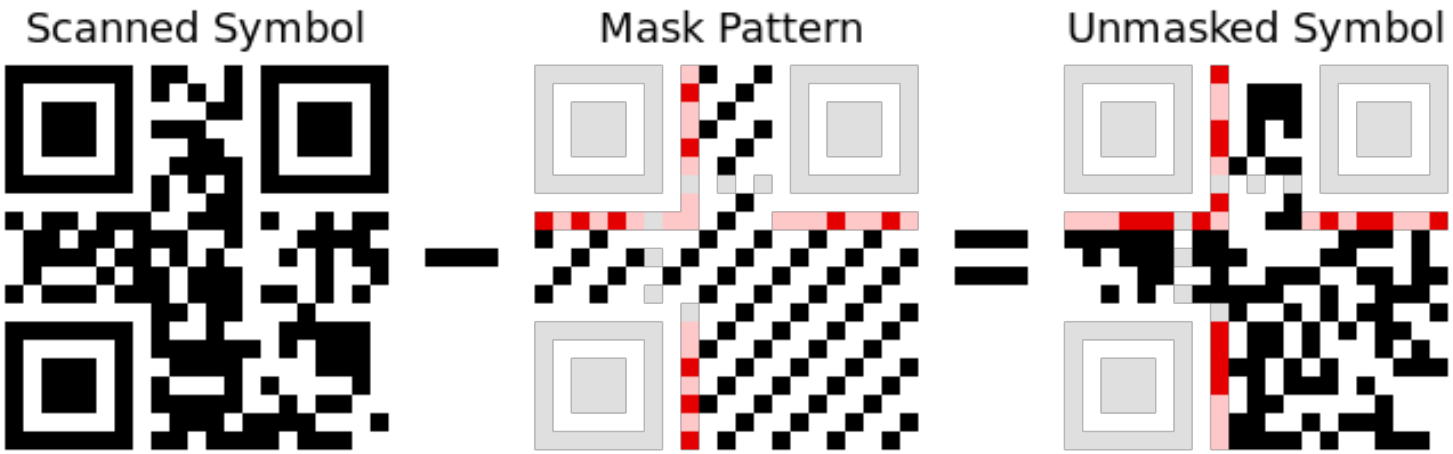
   Lösung des linearen Gleichungssystems.
4. Rekonstruktion von $d(x)$ aus $f(x) - e(x)$
5. Erhalte die Originaldaten als $c(x) := d(x) : g(x)$

Reed Solomon für QR Codes

QR Codes bestehen aus:

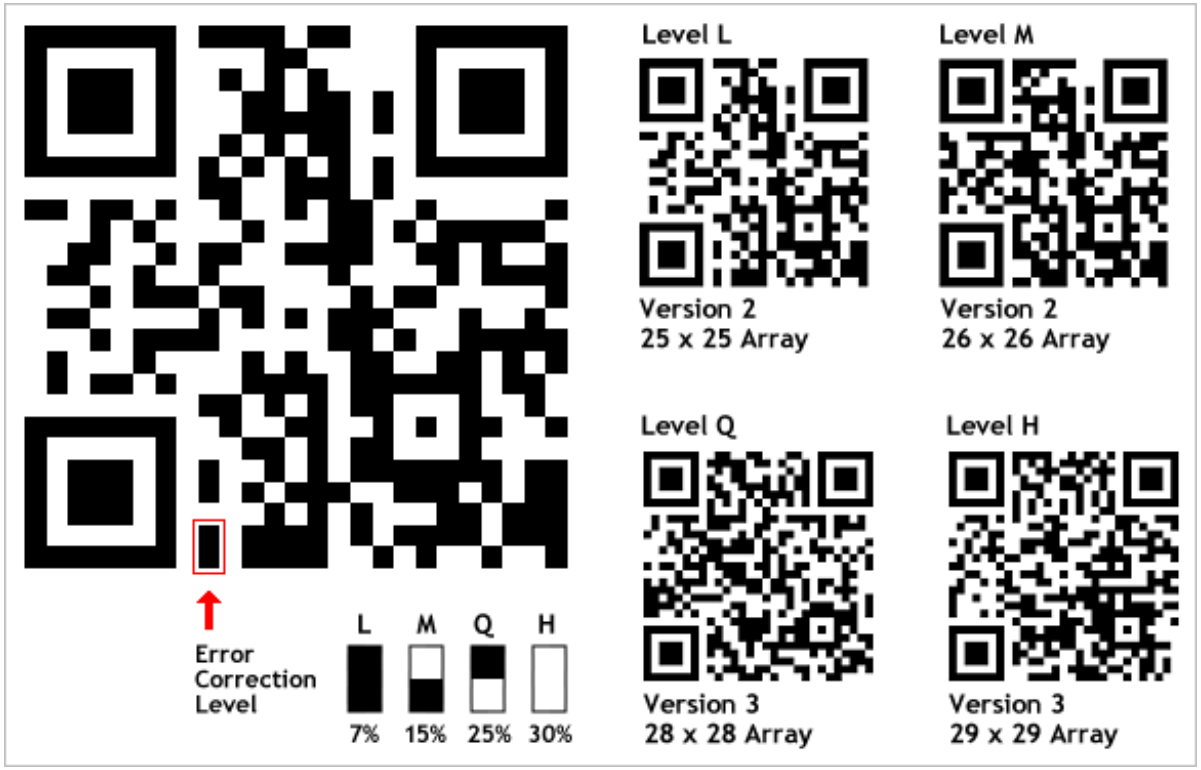
- schwarzen und weissen Quadraten (Interpretation: Bits),
- einem *locator pattern* zur Platzierung des Scanners.

QR Codes



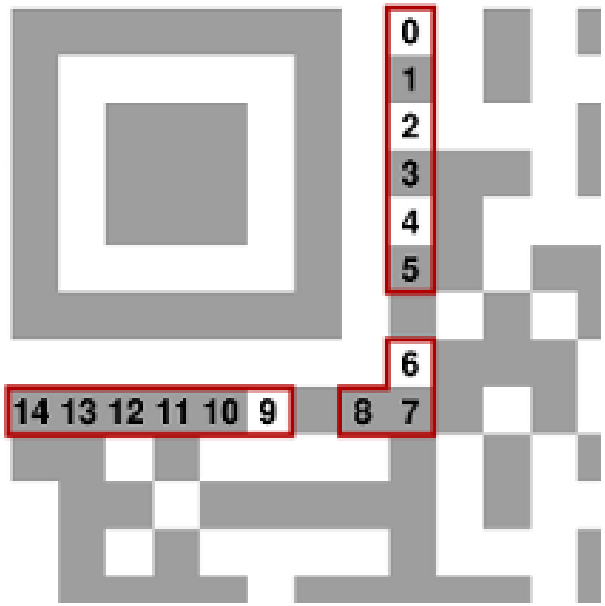
Masking : wird verwendet um Symbole zu maskieren welche den Scanner verwirren könnten, z.B. nehmen weisse Flächen die Stellen der "locator patterns" ein.
Die roten Flächen enkodieren Formatinformationen inklusive der Information welche Maske verwendet wurde und welches Fehler Korrektur Level verwendet wurde. Damit weiss der Scanner erst einmal was er vor sich hat.

QR Codes



Reed Solomon Fehlerkorrektur: Abhängig vom gewaehlten Fehler Korrektur Level kann auch bei beschädigtem QR Code die Gesamtheit der Daten rekonstruiert werden. Bei Level L darf z.B. 7% des QR codes beschädigt sein.

Lesen von QR Codes



Schwarze und weisse Quadrate entsprechen jeweils einem Bit.
Die markierte Sequenz der Bits 0-14 enthält Formatinformation. Von dieser Sequenz enthalten nur 5 Bit (10-14) tatsächlich Information. Der Rest ist für Fehlerkorrektur reserviert. Bits 14 und 13 enthalten das Fehler Korrektur Level und 12,11 und 10 enthalten die Masken ID.

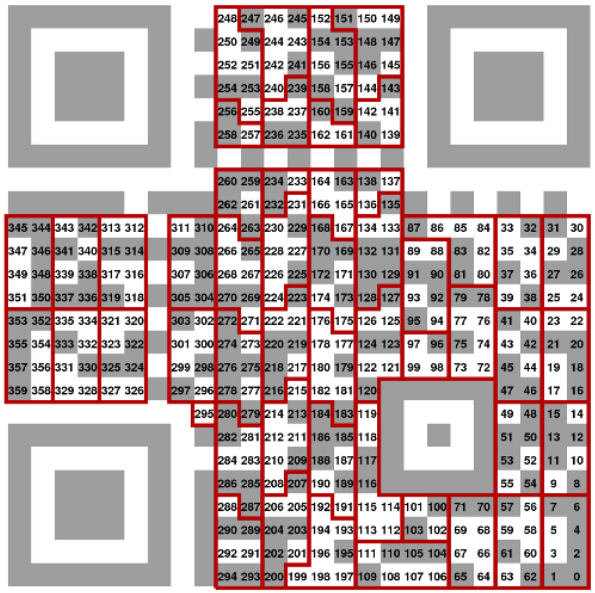
Lesen von QR Codes: Formatinformation

Die oben genannten 15 Bits kann man als Koeffizienten eines Polynoms betrachten deren Koeffizienten entweder 0 oder 1 sind.

$$p(x) = x^14 + x^13 + x^12 + x^11 + x^10 + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x$$

Die eigentliche Information ist in den Termen 10 bis 14 enthalten.
$p(x)$ ist durch das Generatorpolynom $g(x)$ teilbar, damit ist Fehlerkorrektur möglich.

QR Codes: Inhalt



Gruppierungen von je 8 Bits werden zu Bytes zusammengefasst. Wichtig ist hierbei auch die Numerierung die die "Ableserichtung" anzeigt.

References :

http://www.ams.org/samplings/feature-column/fc-2013-02
https://www.cs.cmu.edu/~guyb/realworld/reedsolomon/reed_solomon_codes.html
http://blog.qrstuff.com/2011/12/14/qr-code-error-correction

Vektorräume - Einleitung

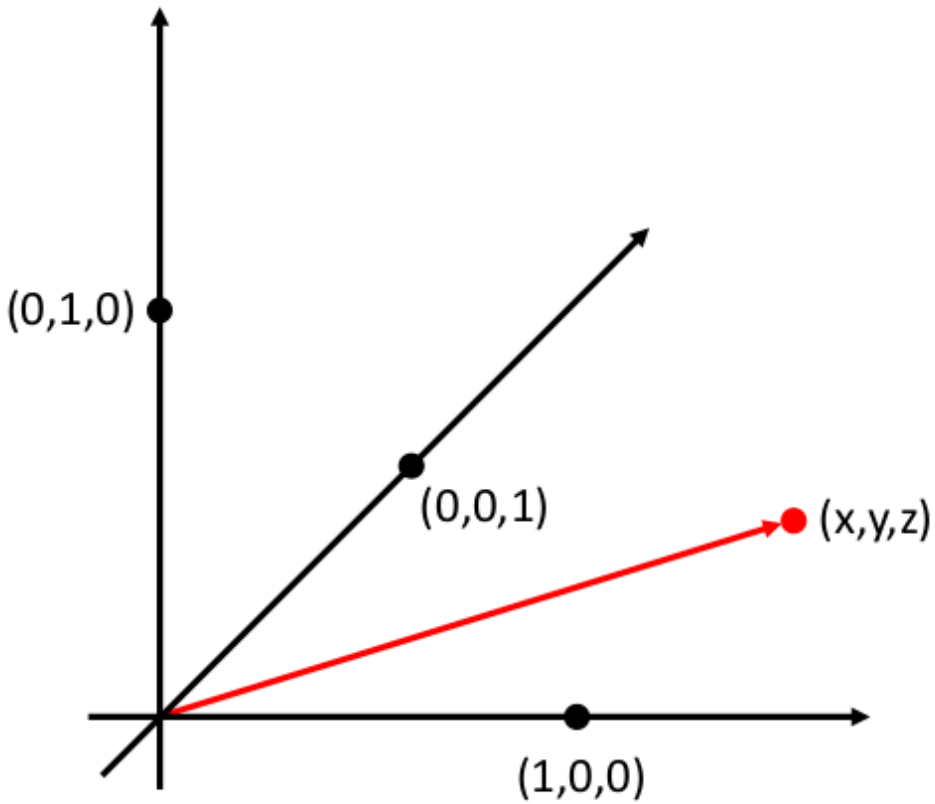
Einleitung

Algebraische Strukturen sind eine sehr mathematische Konstruktion, dh man kann damit rechnen, aber man kann sich wenig drunter vorstellen.

„In der Mathematik versteht man die Dinge nicht.
Man gewöhnt sich nur an sie.“
– John von Neumann

Vektoren und Vektorräume hingegen sind sehr viel einfacher, schlicht weil sie unserem alltäglichen Verständnis entsprechen. Unser drei-dimensionaler Raum kann man einfach als $\mathbb{R}^3$ verstehen und eine Landkarte als $\mathbb{R}^2$.

Vektorraum



Vektorraum

Anmerkungen:
Diese Art Koordinaten aufzuzeichnen nennt man „kartesisches Koordinatensystem“.

double[] x = new double[3]; würde in Java genau einen solchen Vektor in $\mathbb{R}^3$ erzeugen.

Man muss sich nicht auf $\mathbb{R}^2$ oder $\mathbb{R}^3$ beschränken, man kann auch mit $(3, 1, 4, 1, 5, 9, 2, 6, 5, \dots) \in \mathbb{R}^{34}$ arbeiten. Explizit vorstellen kann man es sich halt nicht mehr.

Man kann statt $(1, 2, 3, \dots)$ auch $\begin{pmatrix} 1 \\ 2 \\ 3 \\ \vdots \end{pmatrix}$ schreiben. Das ist Geschmackssache (zumindest fast).

Vektorraum

Man kann auf Vektorräumen natürlich auch Verknüpfungen definieren:

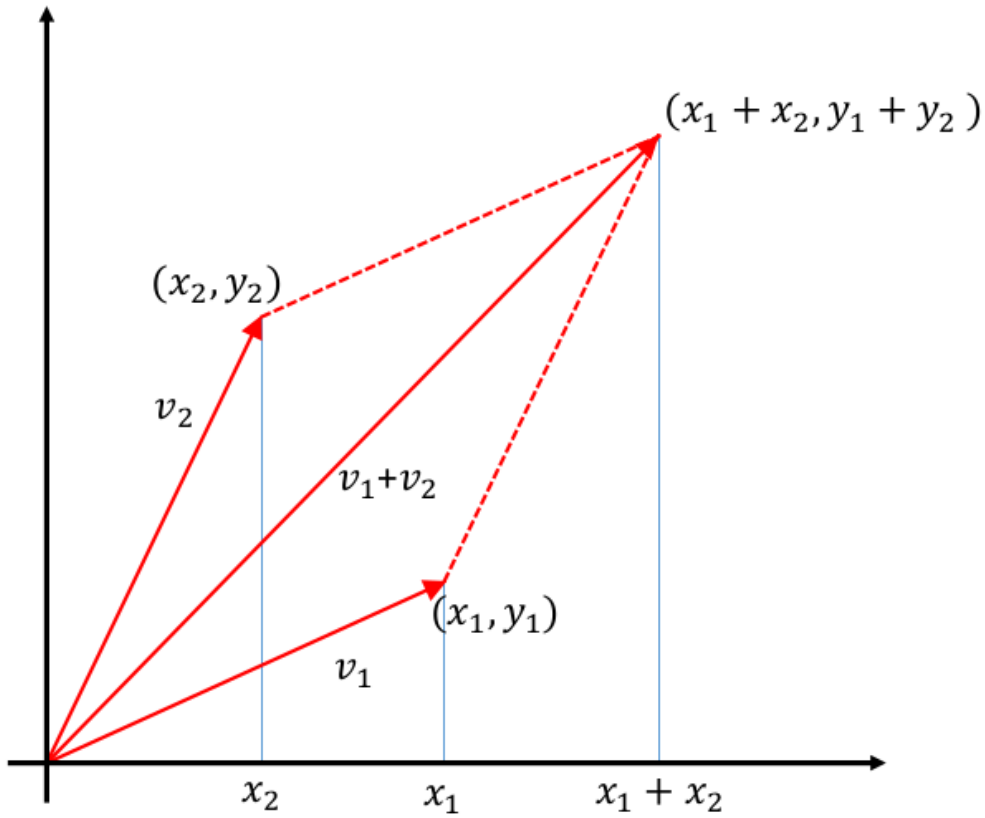
Vektoraddition:

$$v_1 + v_2 = \begin{pmatrix} x_1 \\ y_1 \\ z_1 \\ \vdots \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \\ z_2 \\ \vdots \end{pmatrix} := \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 \\ \vdots \end{pmatrix}$$

Mit einem neutralen Element $(0, 0, 0, \dots)$ bildet das dann eine Gruppe.
$\Rightarrow$ Übungsaufgabe: Beweise das

Man kann das so verstehen, dass der „Pfeil“ v_2 an den „Pfeil“ v_1 dran gehängt wird. Das Ganze kann man sehr schön graphisch darstellen:

Vektorraum



Vektorraum

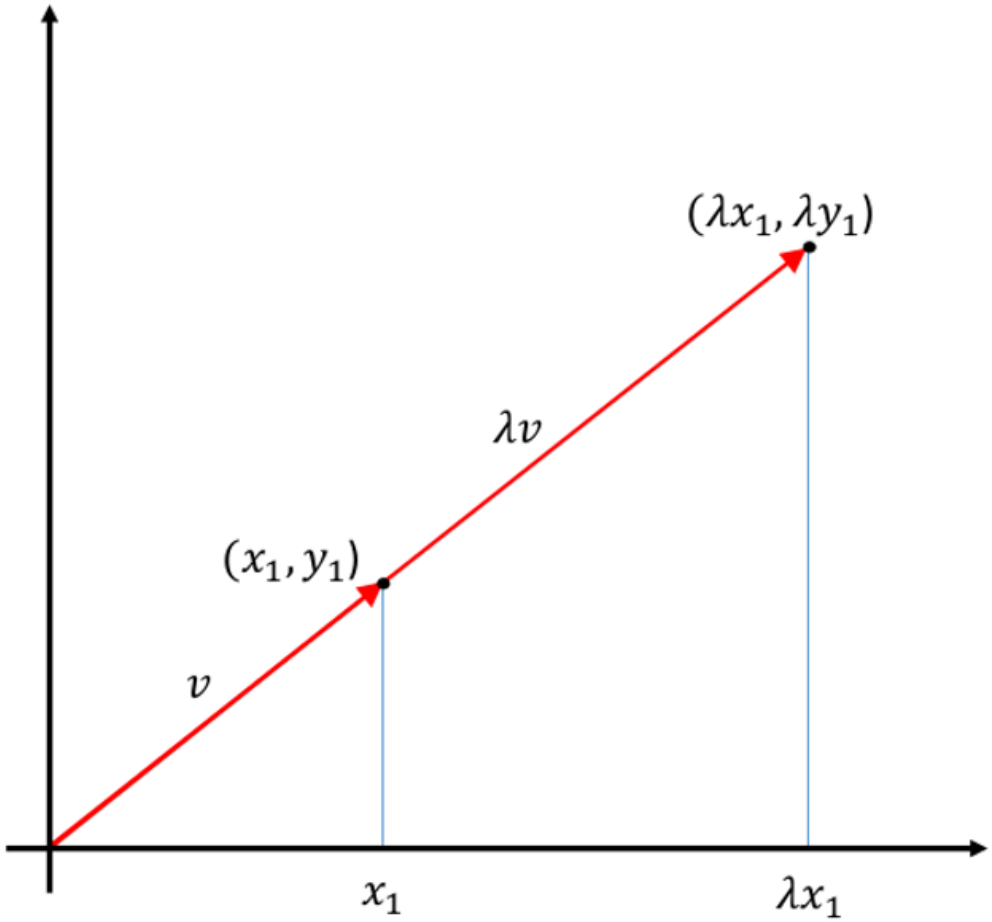
Eine andere sehr wichtige Verknüpfung ist die **Skalarmultiplikation**. Skalarmultiplikation ist die Streckung des Vektors um einen Faktor c.

Definiert wird das so:

$$\lambda v_1 = \lambda \begin{pmatrix} x_1 \\ y_1 \\ z_1 \\ \vdots \end{pmatrix} := \begin{pmatrix} \lambda x_1 \\ \lambda y_1 \\ \lambda z_1 \\ \vdots \end{pmatrix}$$

Wenn $|\lambda| < 1$ ist, dann wird natürlich der Vektor nachher kürzer sein als vorher, dh $|\lambda v_1| < |v_1|$.

Vektorraum



Vektorraum

Wir haben die Verknüpfungen kennen gelernt und nun die Definition:

Definition:
Sei K ein Körper. Ein **Vektorraum** V mit Skalaren aus K besteht aus einer kommutativen Gruppe $(K, +)$ und einer skalaren Multiplikation $\cdot : K \times V \to V, (\lambda, v) \mapsto \lambda \cdot v$, sodass für alle $v, w \in V$, $\lambda, \mu \in K$ gilt:

(V1) $\lambda(\mu v) = (\lambda\mu)v$

(V2) $1 \cdot v = v$

(V3) $\lambda(v + w) = \lambda v + \lambda w$

(V4) $(\lambda + \mu)v = \lambda v + \mu v$

Vektorraum

Anmerkungen:
Wir sehen, dass wir hierfür immer einen Körper K brauchen um von einem Vektorraum sprechen zu können. Wenn $K = \mathbb{R}$ ist sprechen wir von einem **reellen Vektorraum**, wenn $K = \mathbb{C}$ gilt, von einem **komplexen Vektorraum**. Man sagt dann zB Vektorraum über $\mathbb{R}$ oder $\mathbb{R}$-Vektorraum und schreibt $V(\mathbb{R})$.

Man könnte natürlich auch ganz andere Körper verwenden, z. B. den Galois Körper $v \in V(GF(2))$ darstellen, zB $v = (0, 1, 1, 1, 0, 0, 0, 1)$.

Vektorraum

Definition:
Sei V ein K-Vektorraum und $U \subset V$ mit $U \neq \emptyset$. Ist U mit den Verknüpfungen von V selbst wieder ein K-Vektorraum, so heißt U **Untervektorraum** von V. Man sagt auch **Teilraum** oder **Unterraum**.

Satz:
Sei V ein K-Vektorraum und $U \subset V$, $U \neq \emptyset$. U ist genau dann ein Teilraum von V, wenn gilt:

(U1) $u + v \in U$ für alle $u, v \in U$

(U2) $\lambda u \in U$ für alle $\lambda \in K, u \in U$

Diese Bedingungen bedeuten lediglich, dass der Teilraum abgeschlossen ist bzgl. der Verknüpfungen.
Beweis (voraussichtlich) in der Übung.

Vektorraum

Beispiel:
Betrachten wir das ganze anhand des $V = \mathbb{R}^2$. Ein Teilraum U ist uninteressant, wenn er nichts enthält, also haben wir $u \in U$.
Es muss gelten $\lambda u \in U$ für alle $\lambda \in \mathbb{R}$, dh alle Vektoren, die die gleiche Richtung wie u haben.
Wenn wir einen zweiten Vektor $v \in U$ haben, dann ist auch $\mu v \in U$ und nach $(U1)$ auch $\lambda u + \mu v$

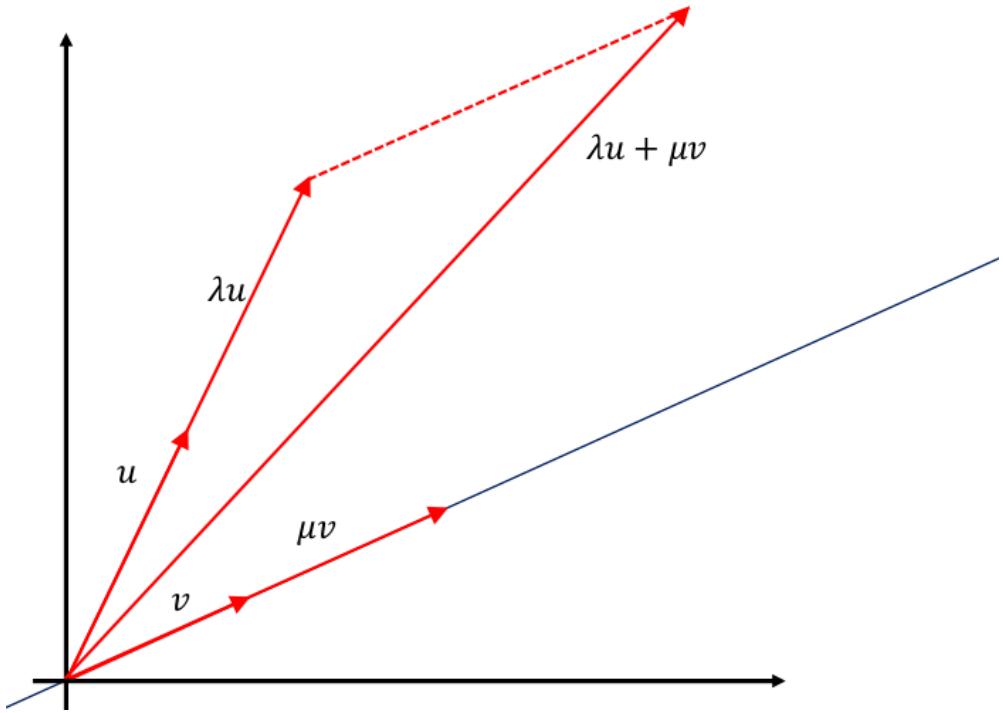
Definition:
Für beliebige u_i, λ_i gilt:

$$\lambda_1 u_1 + \lambda_2 u_2 + \lambda_3 u_3 + \dots$$

ist eine **Linearkombination** von u_i. Und die Menge aller solcher Linearkombinationen ist **Span**$(u_1, u_2, u_3, \dots)$.

Vektorraum

Beispiel:
Der Span(u_i) bildet immer einen Teilraum von V
Man nennt den Span auch oft **Lineare Hülle**



Lineare Abbildungen

Lineare Abbildungen

Lineare Abbildung:
Wir erinnern uns an Homomorphismen zwischen Gruppen. Wenn diese bijektiv sind bedeutet dies, dass die Struktur der Gruppen „gleich“ ist.

Lineare Abbildungen sind das Äquivalent für Vektorräume. Wenn man eine bijektive lineare Abbildung zwischen zwei Vektorräumen hat, dann sind diese im Prinzip ident.

Eine bijektive lineare Abbildung nennen wir „Isomorphismus“ und die Vektorräume sind isomorph. Wir schreiben dafür $U \cong V$

Lineare Abbildungen

Definition:
Es seien U, V Vektorräume über K. Eine Abbildung $f : U \to V$ heißt **lineare Abbildung**, falls für alle $u, v \in U$ und für alle $\lambda \in K$ gilt:

(LA1) $f(u + v) = f(u) + f(v)$

(LA2) $f(\lambda u) = \lambda f(u)$

Lineare Abbildungen

Beispiel:

Betrachten wir: $f : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + x_2 \\ 0 \end{pmatrix}$.

Zu zeigen: 1) Ist dies eine Lineare Abbildung?

(LA1) $f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = f\left(\begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix}\right) = \begin{pmatrix} x_1 + y_1 + x_2 + y_2 \\ 0 \end{pmatrix} =$

$\begin{pmatrix} x_1 + x_2 \\ 0 \end{pmatrix} + \begin{pmatrix} y_1 + y_2 \\ 0 \end{pmatrix} = f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) + f\left(\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right)$

(LA2) $f\left(\lambda \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = f\left(\begin{pmatrix} \lambda x_1 \\ \lambda x_2 \end{pmatrix}\right) = \begin{pmatrix} \lambda x_1 + \lambda x_2 \\ 0 \end{pmatrix} =$

$\lambda \begin{pmatrix} x_1 + x_2 \\ 0 \end{pmatrix} = \lambda f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right)$

Lineare Abbildungen

Beispiel:

Betrachten wir: $f : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + x_2 \\ 0 \end{pmatrix}$.

Zu zeigen: 2) Ist diese Abbildung injektiv/surjektiv/bijektiv?

a) injektiv: Dh wir treffen jeden Punkt maximal einmal.

$f\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $f\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, dh nicht injektiv.

b) surjektiv: Gibt es zB ein Element, das auf $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ abgebildet wird?

Dh $\exists \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 : f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} x_1 + x_2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$? Nein, da $1 \neq 0$ ist.

Lineare Abbildungen

Übungsaufgabe:

Betrachten wir: $f : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$.

Fragen: 1) Ist dies eine Lineare Abbildung?
2) Ist f injektiv?
3) Ist f surjektiv?
4) Ist f bijektiv?

Lineare Abbildungen

Lösung:

1) Ja. (LA1) $f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = f\left(\begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix}\right) = \begin{pmatrix} x_2 + y_2 \\ x_1 + y_1 \end{pmatrix} =$

$\begin{pmatrix} x_2 \\ x_1 \end{pmatrix} + \begin{pmatrix} y_2 \\ y_1 \end{pmatrix} = f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) + f\left(\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right)$

(LA2) $f\left(\lambda \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = f\left(\begin{pmatrix} \lambda x_1 \\ \lambda x_2 \end{pmatrix}\right) = \begin{pmatrix} \lambda x_2 \\ \lambda x_1 \end{pmatrix} =$

$\lambda \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} = \lambda f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right)$

Lineare Abbildungen

Lösung:

2) injektiv: Ang. $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ und $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ wird auf $z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ abgebildet.
Dann gilt $f(x) = f(y) = z$, und damit dann $x_2 = z_1 = y_2$
und $x_1 = z_2 = y_1$, daraus folgt dann $x = y$ und die Abbildung ist injektiv.

3) surjektiv: Wenn wir jetzt mehr über Basen von Vektorräumen wüssten, könnten wir sofort schließen, dass f surjektiv ist, aber so:
Wir suchen ein $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, dass auf $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ abgebildet wird. Suche dir x aus, sodass $x_1 = y_2$ und $x_2 = y_1$ gilt und wir haben es gefunden. Alle Elemente werden getroffen, dh wir sind surjektiv.

4) Ist f bijektiv? Natürlich.

Lineare Abbildungen

Wichtige Anmerkungen:
Wenn wir eine lineare Abbildung $f : U \to V$ haben, die bijektiv, also ein Isomorphismus ist, dann kann man auch die Umkehrabbildung g definieren. Es gilt dann $g = f^{-1}$ und g ist eine lineare Abbildung, die bijektiv ist.

Wenn wir zwei lineare Abbildungen f und g haben, dann ist auch die Verknüpfung $f(g)$ wieder eine lineare Abbildung. Man schreibt dafür $f \circ g$. Man kann zeigen, dass wenn f und g bijektiv sind, dann auch $f \circ g$.

$\Rightarrow$ Beweise dafür in den Repetitorien.